Remarks

The present Response is to the Office Action mailed 10/31/2008, made final. Claims 1-7 and 14-23 are presented for examination.

Detailed Action

1. This action is response to communication: amendment filed on 09/19/2008.

2. Claims 1-7 and 14-23 are currently pending in this application. Claims 1 and 14 are independent claims. Claims 8-13 have been cancelled.

3. No IDS was received for this application.

Response to Arguments

4. Applicant's arguments filed 09/19/2008 have been fully considered but they are moot in view of new ground(s) of rejection

5. The Applicants have amended the claims to recite that a connector, and not a card reader, connects the smart card to a telephone. This however, does not overcome the art. This makes the claims even more broad, and the Landry reference can be read differently.

Claim Rejections - 35 USC § 102

7. Claims 1, 14, and 23 are rejected under 35 U.S.C. 102(e) as being unpatentable over Landry et al US Patent No. 6,687,350 (hereinafter Landry).

As per claim 1, Landry teaches a method for a second operation of authenticating a user and securing an online transaction *over* a telephone, comprising:

providing a connector connecting a smart card to a telephone (Figure 2 item 30, with the analogue front-end unit; col. 5 lines 20-35); transmitting from the smart card at least an identification sequence for the user to an IRV server connected to a telephone line in the form of a modulated signal (col. 10 lines 25-30; col. 5 lines 1-22; col. 6 lines 5-29; Figures 2,3; also col. 5 lines 13-35, wherein the signal is modulated as it goes

through modem 26); demodulating the identification sequence at the IVR server (It is inherent that the signal is demodulated, as a modulated signal must be demodulated in order for the data to be useful and processed; also occurs at the IVR server (col. 5 lines 1-10)); and authenticating the user and the transaction at an application server receiving the demodulated identification sequence from the IVR server over a communication network wherein data processing required for generating, transmitting, and authenticating the user occur without data processing assistance from the connector (col. 8 line 45-65; col. 10 lines 1-35; Figure 5, and abstract, wherein the application server controls the functions of the smart card reader).

Claim 14 is rejected using the same basis of arguments used to reject claim 1 above. A card reader connected to a telephone is taught throughout the reference, such as in Landry Figure 1a and 1b. It is inherent that a telephone is connected to a telephone line. An IVR server connected to the telephone line is taught throughout the reference, such as in Figures 1, 2, 3, and col. 5 lines 1-12.

As per claim 23, Landry teaches wherein the card reader is further integrated into the telephone handset (col. 2 lines 45-68).

Applicant's response:

Applicant has herein amended claim 1 and claim 14 to significantly narrow these claims with further limitations specific to the smart card and the connector. Claim 1 now recites:

1. (Currently amended) A method for authenticating a user and securing an online transaction over a telephone, comprising:

(a) connecting a smart card having a conventional ISO 7816 six pad array and first circuitry to operate as a conventional smart card, further comprising second circuitry enabled to produce a modulated voltage signal modulated in a manner to produce an identification sequence stored on the smart card and associated with a specific person, on one otherwise unused pad once each time the Rst (reset pad) is pulled low by closing a

switch between the Rst pad and Gnd, to a telephone line in a manner that the modulated voltage signal is transmitted on the telephone line;

(b) connecting a telephone hand set to the same telephone line;

(c) connecting to an interactive voice response (IVR) server on the telephone network by dialing an appropriate number on the handset;

(d) entering a pin number through the telephone handset by the specific person, and pressing the switch to pull the Rst low and transmit the modulated identification sequence to the IVR;

(e) demodulating the identification sequence at the IVR, and using the demodulated identification sequence and the PIN to communicate with an authentication server and authenticate the person.

The additional limitations of at least the dual nature of the smart card, presenting the identification sequence as a modulated voltage signal on the otherwise unused pad of the ISO 7816 array by pulling the Rst pad by closing a switch in a connector, the switch between the Rst pad and Gnd, which transmits the sequence to an IVR, render this amended claim patentable over Landry, as Landry teaches none of these limitations.

Claim 14 now recites:

14. (Currently amended) A system for authenticating ~~a user~~ and securing online transactions for a user over a telephone, comprising;

a smart card having a conventional ISO 7816 six pad array and first circuitry to operate as a conventional smart card, further comprising second circuitry enabled to produce a modulated voltage signal modulated in a manner to produce an identification sequence stored on the smart card and associated with a specific person, on one otherwise unused pad once each time the Rst (reset pad) is pulled low by closing a switch between the Rst pad and Gnd, to a telephone line in a manner that the modulated voltage signal is transmitted on the telephone line;

a connector connecting the one pad on which the modulated signal is produced, the Gnd pad, aVbb pad, and the Rst pad of the ISO pad array to the telephone line, with a normally-open switch imposed between the Rst pad and Gnd;

a telephone connected on the telephone line;

an interactive voice response (IVR) server connected to the telephone line; and

an authentication server connected to the IVR server over a communication network;

wherein upon the specific person opening a connection to the IVR by dialing an appropriate number by the handset, entering a PIN, and closing the normally open switch to cause the identification sequence to be transferred to the IVR, the IVR demodulates the identification sequence, and uses the demodulated identification sequence and the PIN to communicate with the authentication server and authenticate the person.

The additional limitations in amended claim 1 are the same as the additional limitations in claim 14 by amendment, and the same reasoning applies as to why claim14 is now patentable over Landry.

Claim Rejections - 35 USC § 103

9. Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Landry as applied above, and further in view of Chang et al. US Patent No. 6,715,082 (hereinafter Chang).

As per claim 2, Landry teaches a credit card number in col. 1 lines 25-29, which is a unique number. However, Landry and Brown do not explicitly teach the use of one time keys on a smart card. These are well known in the art, as can be seen in Chang col. 2 lines10-25.

At the time of the invention, it would have been obvious to include random onetime keys to be stored on smart cards. One of ordinary skill in the art would have been

motivated to perform such an addition to increase security. This is taught by Chang in col. 2 lines 11-15.

As per claim 3, the one-time password taught by Chang in col. 2 lines 10-25 is a key used in a session. It is taught in Chang that this one time password/key is not transmitted to an authentication server, as it is only transmitted to an access server.

Claim 15 is rejected using the same basis of arguments used to reject claim 2 above.

Claim 16 is rejected using the same basis of arguments used to reject claim 3 above.

10. Claims 4 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Landry and Chang as applied above, and further in view of Brinkmeyer et al. US Patent No. 5,619,573 (hereinafter Brink).

As per claim 4" the Landry combination does not explicitly teach wherein the session key is a function of a previous key. However, this is taught by Brink, such as in col. 3 lines 60 to col. 4 line 25. This would be inherently known by an authentication server, as the authentication server needs to know the key in order to verify if it was valid or not.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include using a previously known key. One of ordinary skill in the art would have been motivated to perform such an addition to create more security. As they are one way functions, it would be extremely difficult to determine the previous keys unless they were known. By using previous keys, it would increase security, as it would almost guarantee that the key was actually known by the user and the authentication server, and not a malicious middle man.

Claim 17 is rejected using the same basis of arguments used to reject claim 14 above.

11. Claims 5-7 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Landry, Chang, and Brink as applied above, and further in view of Bruce Schneier's Applied Cryptography, 2nd Edition (1997), (hereinafter Schneier).

As per claims 5-7, the claims recite the use of encryption keys, decryption, one-way functions and authentication. These are well known in the art, as taught throughout Schneier, such as in pages 28-42. Pin codes are taught throughout Landry and Kia, and it would be obvious to encrypt PIN's, because PIN contains sensitive information, which should never be sent in the clear. Further, it is common practice that authentication is valid if PIN's match a PIN stored in a database. (That's how PIN's or passwords work). Further, databases holding security information is taught throughout Kia, such as in col. 2 lines 14-20 and in col. 3 lines 15-24 and col. 4 lines 29-37.

At the time of the invention, it would have been obvious to combine the teachings of Schneier with the Landry combination. One of ordinary skill in the art would have been motivated to perform such an addition to be able to provide a secure system. The Landry combination is already directed to secure online transactions, and Schneier teaches the details of this.

Claim 18-20, as best understood by the Examiner, are rejected using the same basis of arguments used to reject claims 507 above.

12. Claims 21-22 are rejected under 35 U.S.C. 103(a) as being obvious over Landry and as applied above.

As per claim 21, the claim recites wherein the smart card is powered by the voltage provided by the telephone line. It is well known in the art that telephones are powered by the power flowing from telephone lines. Since the Smart Card reader is attached to the telephone, as taught in Landry, it would have been obvious to power a smart card that is connected to the phone using the voltage provided by the phone, as this would reduce the amount of more power sources and voltage lines. Further, Landry teaches that the smart card may be powered by the telephone set, in col. 7 lines 50-54. As already discussed, many phones are powered by the telephone lines.

As per claim 22, it is inherent that a smart card would transmit signals via contacts. Although the Landry combination does not explicitly teach ISO contacts, it would have been obvious to do so, if not inherent. As Landry already teaches utilizing contacts, it would have been obvious to utilize ISO contacts, as ISO contacts are well

known in the art and used throughout industry. It would have been obvious incorporate ISO contacts for ease of use.

Applicant's response:

As claims 1 and 14 are now patentable, claims 2-13, depended from claim 1, and claims 15-23, depended from claim 14 are all patentable at least as depended from a patentable claim.

Summary

As all of the claims, as amended and argued above, have been shown to be patentable over the art presented by the Examiner, applicant respectfully requests reconsideration and the case be passed quickly to issue.

If any fees are due beyond fees paid with this amendment, authorization is made to deduct those fees from deposit account 50-0534. If any time extension is needed beyond any extension requested with this amendment, such extension is hereby requested.

Respectfully Submitted,
Vincent Cedric Colnot

By */Donald R. Boys/*
Donald R. Boys
Reg. No. 35,074

Central Coast Patent Agency, Inc.
3 Hangar Way, Suite D
Watsonville, CA 95076
831-768-1755